



Netwatch

By Jim Carroll

Your guide to business & accounting on the Internet

What evil lurks in e-mail?

I have always been of two minds when it comes to the retention of e-mail messages. If there is any kind of potential smoking gun in the information age, it has to be electronic mail. However, a personal e-mail archive can also be an incredibly powerful knowledge tool.

E-mail retention is receiving closer scrutiny than ever before, with many legal disputes involving electronic records, including e-mail archives. Our rapidly evolving regulatory environment, which has many new policies concerning corporate record retention, is now dragging e-mail into its net. And clearly there has been an increasing number of embarrassing — not to mention

legally risky — situations involving the leakage of corporate e-mail messages.

Consider the legal mess Credit Suisse First Boston found itself in after e-mail messages were discovered from its “star” telecom analyst, Frank Quattrone, suggesting a cleanup of certain corporate records. And then there were several internal e-mails from Merrill Lynch,

obtained during a legal discovery process, in which analysts and staff appeared to be privately trashing various stocks they were recommending to the public. How big is the risk of errant e-mail messages becoming public? Visit Internal Memos — a website of purported internal e-mail messages and other documents — and you’ll discover that such risk increases on a daily basis.

One problem is the very nature of e-mail: it is so easy to use and so informal that employees will often commit something to an e-mail that they would never put on paper. E-mail messages can be quickly forwarded to dozens of people, including individuals outside the company, and can be saved for future use. Any one of those copies could be a case breaker in a legal action, or at the very least a significant public relations problem if leaked to the outside world. That’s why, if you haven’t already done so, you should develop and implement a clear and concise policy pertaining to corporate

e-mail. This includes guidance to staff about the types of messages that should be retained, what should be destroyed, and on what schedule this should occur. There should also be a clear position on whether individual e-mail records are per-

mitted. Furthermore, the policy should define how e-mail records will be backed up and accessed.

This policy needs to work within the context of our current regulatory environment, so proper legal advice should be obtained. Also, to ensure the policy is properly implemented and adequately enforced, an ongoing audit is required. This means extensive education of all staff regarding the nature and reasons for the policy.

How should you go about creating a policy? Aside from direct legal advice, you can obtain information through a variety of online resources pertaining to records retention issues, such as the Association for Information Management Professionals. In addition to a number of useful articles, you’ll find it has several books, including *Guideline for Managing E-mail* (US\$34).

With a bit of research, you can find fairly extensive corporate policies online, such as the State of California Electronic Records Management Handbook, or documents at email-policy.com. Finally, GigaLaw has a very useful article on the legal issues of e-mail.

Jim Carroll, FCA, is a well-known speaker, author and columnist. Reach him at jcarroll@jimcarroll.com or log on to his website at www.jimcarroll.com

E-MAIL POLICY ONLINE

Association for Information Management Professionals www.arma.org

State of California Electronic Records Management Handbook www.pd.dgs.ca.gov/recs/erm-toc

Internal Memos www.internalmemos.com/memos

E-Mail Policy www.email-policy.com

GigaLaw article www.gigalaw.com/articles/2002/towns-2002-01